1МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт профессионального образования

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: ректорат
Должность: проректор по среднему профессиональному образованию
Дата: 17.05.2023 11:27:42

Попов Иван Павлович

Программа производственной практики

по профессиональному модулю
«Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Присваиваемая квалификация
"Техник по защите информации "

Формы обучения
очная

Кемерово 2022 г.

1699402314

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 16.05.2023 05:43:52

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 3/1 от 16.05.2023

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 16.05.2023 02:45:40

Прокопенко Евгения Викторовна

Согласовано цикловой-методической комиссией по направлению подготовки (специальности) 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Протокол № 4/1 от 16.05.2023

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 16.05.2023 04:34:39

Прокопенко Евгения Викторовна

Согласовано заместителем директора по УР ИПО

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: Заместитель директора по учебной работе
Дата: 16.05.2023 04:34:39

Полуэктова Наталья Сергеевна

Согласовано заместителем директора по МР ИПО

1. Общая характеристика рабочей программы практики

Производственная практика является частью программы подготовки профессинального модуля «Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин» основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Прохождение практики направлено на формирование компетенций:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации;
Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;
Иметь практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
Иметь практический опыт: установка, настройка программных средств защиты информации в автоматизированной системе;

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
Уметь: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
Иметь практический опыт: обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети;

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
Знать: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
Уметь: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
Иметь практический опыт: тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
Знать: особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
Уметь: применять средства гарантированного уничтожения информации;
Иметь практический опыт: учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности;

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Знать: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;
Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
Иметь практический опыт: работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе;

2. Структура и содержание рабочей программы практики

2.1 Объем практики и виды работы

Вид учебной работы	Объем часов
Обязательная нагрузка (всего)	**108 часов**
Промежуточная аттестация в форме .	

2.2 Тематический план и содержание практики

Наименование тем практики	Виды работ	Объем часов
Вид профессиональной деятельности: Защита информации в автоматизированных системах программными и программноаппаратными средствами		
	Консультация	2
Программные и программноаппаратные средства защиты информации. Криптографические средства защиты информации.	Анализ принципов построения систем информационной защиты производственных подразделений.	16
	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	16
	Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	16
	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	18
	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	20
	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	20
Всего:		108

3. Условия реализации программы практики

3.1 Требования к минимальному материально-техническому обеспечению

Оборудование рабочих мест:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональный компьютер.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3. Специальное помещение № 1251 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

4. Специальное помещение № 1139 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

5. Специальное помещение № 1147 представляет собой помещение для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь

Помещение для самостоятельной работы обучающихся:

6. Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Помещение для самостоятельной работы обучающихся:

7. Специальное помещение № 1211 представляет собой помещения для самостоятельной работы,

оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

8. Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:

Перечень основного оборудования:

Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры

Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk

Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,

СПРУТ-ОКП

9. Специальное помещение №1251 представляет собой лабораторию программных и программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами; программно-аппаратными средствами защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности; программными и программно-аппаратными средствами обнаружения вторжений; средствами уничтожения остаточной информации в запоминающих устройствах; программными средствами выявления уязвимостей в автоматизированных системам и средствах вычислительной техники; программными средствами криптографической защиты информации; программными средствами защиты среды виртуализации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Батаев, А. В. Операционные системы и среды : учебник для образовательных учреждений среднего профессионального образования по укрупненной группе специальностей "Информатика и вычислительная техника" / А. В. Батаев, Н. Ю. Налютин, С. В. Синицын ; А. В. Батаев, Н. Ю. Налютин, С. В. Синицын. – 5-е издание переработанное – Москва : Академия, 2021. – 285 с. с. – (Профессиональное образование : Информатика и вычислительная техника). – URL: https://academia-moscow.ru/reader/?id=539321 (дата обращения: 26.09.2023). – Текст : электронный.

3.2.2 Дополнительная литература

1. Рудаков, А. В. Операционные системы и среды : Учебник для СПО / А. В. Рудаков. – Москва : НИЦ ИНФРА-М, 2024. – 304 с. – ISBN 978-5-906923-85-1. – URL: https://znanium.com/catalog/document?id=430571 (дата обращения: 26.09.2023). – Текст : электронный.

3.2.3 Методическая литература

1. Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 290 с. – URL: http://library.kuzstu.ru/meto.php?n=9964 (дата обращения: 26.09.2023). – Текст : электронный.

2. Методические указания по оформлению отчетов по практике, курсовых работ (проектов) и выпускных квалификационных работ : для всех специальностей СПО / Кузбасский государственный

технический университет им. Т. Ф. Горбачева ; Кафедра информатики и информационных систем, составители: Н. С. Полуэктова, Т. С. Семенова. – Кемерово : КузГТУ, 2022. – 1 файл (762 Кб). – URL: http://library.kuzstu.ru/meto.php?n=10478 (дата обращения: 26.09.2023). – Текст : электронный.

3.2.4 Ресурсы информационно-телекоммуникационной сети «Интернет»

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.

10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. Фонд оценочных средств

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по производственной практике по профессиональному модулю "Защита информации в автоматизированных системах программными и программноаппаратными средствами"

4.1. Паспорт фонда оценочных средств

Планируемые результаты обучения по практике.

Практика направлена на формирование следующих компетенций выпускника:

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Защита информации в автоматизированных системах программными и программноаппаратными средствами	ПК 2.1	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Практический опыт:** установка, настройка программных средств защиты информации в автоматизированной системе;	Проверка отчёта по разделам практики.
	ПК 2.2	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **Умения:** устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Практический опыт:** обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети;	Проверка отчёта по разделам практики.
	ПК 2.3	**Знания:** методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; **Умения:** диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; **Практический опыт:** тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;	Проверка отчёта по разделам практики.
	ПК 2.4	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; **Умения:** применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; **Практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;	Проверка отчёта по разделам практики.
	ПК 2.5	**Знания:** особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; **Умения:** применять средства гарантированного уничтожения информации; **Практический опыт:** учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности;	Проверка отчёта по разделам практики.
	ПК 2.6	**Знания:** типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; **Практический опыт:** работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе;	Проверка отчёта по разделам практики.

4.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

4.2.1. Оценочные средства при текущем контроле

Текущий контродь по производственной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

90-100 баллов – при раскрытии всех разделов в полном объеме;
80-89 баллов – при раскрытии всех разделов с недочетами;
60-79 баллов – при раскрытии не всех разделов в полном объеме;
0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Анализ принципов построения систем информационной защиты производственных подразделений

Задание 1. Изучите инфраструктуру комплекса АИС, АРМ, включая сетевую инфраструктуру.

Задание 2. Изучите требования и правила, действующие в производственных подразделениях с точки зрения информационной защиты.

Задание 3. Выпишите для себя наиболее «слабые места» с точки зрения информационной защиты и возможные угрозы.

Задание 4. Сформируйте перечень мероприятий для усиления наиболее «слабых мест» с точки зрения информационной защиты.

Тема 1.2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.

Задание 1. Ознакомьтесь с инструкцией по эксплуатации элементов программной защиты автоматизированной системы. Проверьте условия эксплуатации программной защиты – наличие конфликтующего ПО, установку всех необходимых обновлений ОС.

Задание 2. Ознакомьтесь с инструкцией по эксплуатации элементов аппаратной защиты автоматизированной системы. Проверьте условия эксплуатации аппаратной защиты – качество питающего напряжения, заземления, экранирования.

Задание 3. Проверьте исправность элементов охлаждения и отсутствия в них скоплений пыли, при необходимости произведите чистку и смазку вентиляторов.

Задание 4. Зафиксируйте в журнал выполненные работы.

Тема 1.3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.

Задание 1. Ознакомьтесь с инструкцией по эксплуатации элементов программной защиты автоматизированной системы. По заданию наставника проверьте наличие актуальных обновлений, при необходимости установите их. Проанализируйте системные журналы программных средств защиты на предмет ошибок.

Задание 2. Ознакомьтесь с инструкцией по эксплуатации элементов аппаратной защиты автоматизированной системы. По заданию наставника проверьте качество всех соединений. При наличии большого количества пыли выполните очистку оборудования.

Задание 3. Пронаблюдайте за действиями наставника по тестированию комплекса программно-аппаратных средств обеспечения информационной безопасности.

Задание 4. С помощью соответствующих приборов и инструментов проверьте качество питающей сети, заземления, а также надежность изоляции и экранирования.

Задание 5. При наличии замеченных дефектов в пунктах 1-4 зафиксируйте их и предложите способы их устранения.

Задание 6. После устранения выявленных дефектов под наблюдением наставника выполните повторное тестирование комплекса программно-аппаратных средств информационной защиты и сделайте соответствующую запись в журнале обслуживания.

Тема 1.4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении

Задание 1. Ознакомиться с типами и особенностями применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.

Задание 2. При наличии нескольких возможных или дублирующих средств защиты поочередно провести с каждым из них тестирование с имитацией информационных угроз. Записать все полученные результаты.

Задание 3. На основании полученных результатов сделать вывод об эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. Принять решение об использовании выбранного наиболее эффективного средства и отказе от наименее эффективных средств.

Тема 1.5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации

Задание 1. Ознакомиться с основными правилами учета, обработки, хранения и передачи конфиденциальной информации на примере определенного учреждения.

Задание 2. Проанализировать возможные угрозы информационной безопасности на каждом этапе этих процедур.

Задание 3. Сформировать и показать наставнику список возможных угроз, выполнить их классификацию по способам реализации и степени опасности, а также предложить варианты защиты от этих угроз.

Задание 4. После согласования угроз и методов защиты от них прослушать инструктаж, проводимый наставником для сотрудников учреждения.

Тема 1.6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.

Задание 1. Изучить нормативно-правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами, применяемыми в данном учреждении.

Задание 2. Изучить внутренние правила и инструкции учреждения по обеспечению информационной безопасности программно-аппаратными средствами.

Задание 3. Найти несоответствия между нормативными и внутренними документами, выяснить причину несоответствия и предложить варианты устранения этих несоответствий.

4.2.2. Оценочные средства при промежуточном контроле (зачет, диффиринцированный зачет)

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Анализ принципов построения систем информационной защиты производственных подразделений.

1. Что относится к инфраструктуре комплекса АИС, АРМ?

2. Какие вы знаете системы информационной защиты, использующиеся в производственных подразделениях?

3. Что понимается под принципами построения систем информационной защиты производственных подразделений?

4. Сформулируйте кратко основные принципы построения систем информационной защиты

производственных подразделений.

5. На основе каких критериев можно выполнить анализ принципов построения систем информационной защиты производственных подразделений и сделать вывод об их эффективности?

Тема 1.2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.

1. Что относится к условиям эксплуатации элементов программной защиты автоматизированной системы?

2. Что относится к условиям технической эксплуатации элементов аппаратной защиты автоматизированной системы?

3. Какие аппаратные элементы системы защиты нуждаются в периодическом обслуживании?

4. Возможна ли эксплуатация элементов программной и аппаратной защиты автоматизированной системы при несоответствии какого-либо параметра? И если да, то при каких условиях?

5. Существуют ли какие-либо определенные сроки эксплуатации элементов программной и аппаратной защиты автоматизированной системы?

Тема 1.3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.

1. Какие ошибки в работе программно-аппаратных средств обеспечения информационной безопасности указываются в системном журнале?

2. Нужна ли какая-то группа допуска или особое разрешение при выполнении таких работ, как например, удаление пыли из аппаратных элементов средств обеспечения информационной безопасности?

3. Что представляют собой тесты и процедура тестирования комплекса программно-аппаратных средств обеспечения информационной безопасности?

4. Какие приборы и инструменты используются при оценке качества питающей сети, заземления, а также надежности изоляции и экранирования?

5. Какие можно делать выводы на основании записей в журнале обслуживания программно-аппаратных средств обеспечения информационной безопасности?

Тема 1.4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.

1. Как и с помощью чего производится тестирование с имитацией информационных угроз?

2. Как классифицируются типы применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении?

3. Какие критерии используются для оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении?

4. Чем следует руководствоваться при принятии решения по выбору используемого программно-аппаратного средства обеспечения информационной безопасности в структурном подразделении?

5. В каком виде для руководства предприятия удобнее представить результаты анализа эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении?

Тема 1.5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

1. На что следует обратить внимание при изучении правил учета, обработки, хранения и передачи конфиденциальной информации на примере определенного учреждения?

2. Какие возможны виды угроз в процессах учета, обработки, хранения и передачи конфиденциальной информации?

3. Какие мероприятия могут снизить вероятность угроз в процессах учета, обработки, хранения и передачи конфиденциальной информации?

4. Какими основными принципами следует руководствоваться при разработке (либо модернизации) правил учета, обработки, хранения и передачи конфиденциальной информации?

5. Какие основные требования предъявляются к системе учета и мониторинга процессов обработки, хранения и передачи конфиденциальной информации?

Тема 1.6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики

1. Какие существуют нормативно-правовые акты по обеспечению информационной безопасности программно-аппаратными средствами?

2. Какие существуют нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами?

3. Кто разрабатывает локальные нормативные документы по обеспечению информационной безопасности программно-аппаратными средствами на данном предприятии?

4. Кто контролирует исполнение правил по обеспечению информационной безопасности программно-аппаратными средствами на данном предприятии?

5. Если имеются некоторые противоречия между государственными и локальными нормативными документами по обеспечению информационной безопасности программно-аппаратными средствами на данном предприятии, то какие документы имеют приоритет?

4.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта, необходимых для формирования соответствующих компетенций

По итогам практики аттестуются обучающиеся, выполнившие программу практики и представившие индивидуальные отчеты по практике.

Формой итогового контроля прохождения практики является зачет с оценкой.

Зачет проводится с учетом защиты отчетов, составленных в соответствии с требованиями программы практики, на основании утвержденного задания на практику.

Защита отчета проводится руководителем практики от кафедры.

При проведении текущего контроля обучающийся представляет выполненные элементы (разделы) отчета по практике.

Преподаватель анализирует их содержание на соответствие, после чего оценивает достигнутый результат.

При проведении промежуточной аттестации обучающийся представляет отчет по практике.

Преподаватель анализирует содержание отчета, затем путем беседы с обучающимся выявляет его способность обосновывать принятые решения.

5. Иные сведения и (или) материалы

Отчет по практике является основным документом, характеризующим работу обучающегося во время практики. Отчет составляется в соответствии с программой практики и содержит следующие разделы:

1. Титульный лист.
2. Рабочий график (план) практики, утвержденный заведующим кафедрой и согласованный с руководителем практики от КузГТУ и (или) предприятия.
3. Введение.
4. Выполнение индивидуального задания.
5. Выводы.
6. Список использованных источников и литературы.

Требования к оформлению отчета

Результаты практики должны быть оформлены в форме отчета, в соответствии с требованиями:

Страницы не обводятся в рамках, поля не отделяюся чертой. Размеры полей не менее: левого - 30 мм, правого - 10 мм, верхнего - 20 мм и нижнего - 20 мм. Нумерация страниц отчета - сквозная: от титульного листа до последнего листа приложений.

Номер страницы на титульном листе не проставляют.

Номер страницы ставят в центре нижней части листа, точка после номера страницы не ставится.

Страницы, занятые таблицами и иллюстрациями, включают в сквозную нумерацию.

Объем отчета по практике должен быть не менее 16 страниц (без учета приложений) машинописного текста (шрифт 14пт, Times New Roman, через 1 интервал). Отчет должен быть отпечатан на формате А4 и подшит. Описания должны быть сжатыми. Объем приложений не регламентируется, а их содержание определяется обучающимся самостоятельно.

Оформление формул

Формулы должны быть оформлены в редакторе формул. В формулах в качестве символов следует применять обозначения, установленные соответствующими государственными стандартами. Расчет по формулам ведется в основных единицах измерения, формулы записываются следующим образом: сначала записывается формула в буквенном обозначении, после знака равенства вместо каждой буквы подставляется ее численное значение в основной системе единиц измерения; затем ставится знак равенства и записывается конечный результат с единицей измерения. Пояснения символов и числовых

коэффициентов, входящих в формулу, если они не пояснены ранее в тексте, должны быть приведены непосредственно под формулой. Пояснения каждого символа следует давать с новой строки в той последовательности, в которой символы приведены в формуле. Первая строка пояснения должна начинаться со слова «где» без двоеточия после него.

Переносить формулы на следующую строку допускается только на знаках выполняемых операций, причем знак в начале следующей строки повторяют. При переносе формулы на знаке умножения применяют знак «×».

Формула нумеруется, если далее по тексту она будет востребована. Формулы, за исключением формул, помещаемых в приложении, должны нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Допускается нумерация в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой.

Ссылки в тексте на порядковые номера формул дают в круглых скобках, например, в формуле (9.1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией, арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения. Например, формула (А.1).

Оформление иллюстраций

Иллюстрационный материал может быть представлен в виде схем, графиков и т.п. Иллюстрации, помещенные в тексте и приложениях отчета, именуются рисунками.

Иллюстрации выполняются в графических редакторах и располагаются после первой ссылки на них и как можно ближе к ссылке на них в тексте.

Иллюстрации, за исключением иллюстраций приложений, следует нумеровать арабскими цифрами в пределах раздела, либо сквозной нумерацией. Например, «Рисунок 1», «Рисунок 1.1», «Рисунок 2.1».

Ссылку на иллюстрацию дают в следующем виде: «в соответствии с рисунком 1».

Иллюстрация при необходимости может иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок" и наименование помещают после пояснительного текста без точки в конце.

Все рисунки формата большего, чем А4, выносятся в приложения.

Построение таблиц

Слово «Таблица», ее номер и название помещают слева над таблицей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Название таблицы записывают через тире после слова «Таблица» с прописной буквы без точки в конце. Например: «Таблица 2.1 – Технические данные».

Заголовки граф и строк таблицы пишутся с прописной буквы, а подзаголовки граф- со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставят. Заголовки и подзаголовки граф указывают в единственном числе.

Заголовки граф записывают параллельно строкам таблицы. При необходимости допускается перпендикулярное расположение заголовков граф.

Таблицу в зависимости от ее размера помещают под текстом, в котором впервые дана ссылка на нее, или на следующей странице, а при необходимости, в приложении к документу. Допускается помещать таблицу вдоль длинной стороны листа документа.

Если в конце страницы таблица прерывается, ее продолжение помещают на следующей странице. При переносе таблицы на другую страницу название помещают только над первой частью таблицы. Слово «Таблица» указывают только один раз слева над первой частью таблицы а, над другими частями пишут слова «Продолжение таблицы» с указанием номера таблицы.

Все таблицы, за исключением таблиц приложений, нумеруются арабскими цифрами сквозной нумерацией. Допускается нумеровать таблицы в пределах раздела. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенного точкой.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавления перед цифрой обозначения приложения, например, «Таблица А.1», если она приведена в приложении А.

На все таблицы документа должны быть приведены ссылки в тексте, при ссылке слово «таблица» пишется полностью с указанием ее номера.

Оформление списка литературы

Список литературы является обязательным (ненумерованным) разделом отчета, оформляется в

соответствии с ГОСТ 7.1-2003 "Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления", включается в содержание отчета.

Список должен содержать сведения обо всех источниках, использованных при составлении отчета. Располагать источники в списке рекомендуется в порядке появления ссылок в тексте. Возможно и другое разрешенное нормативными документами расположение источников в списке.

Оформление приложений

Приложения оформляют как продолжение отчета и помещают в конце отчета в порядке ссылок на них в тексте. В тексте отчета на все приложения должны быть даны ссылки. Каждое приложение следует начинать с нового листа с указанием на верху посредине страницы слова «ПРИЛОЖЕНИЕ» и его обозначения, например, «ПРИЛОЖЕНИЕ А». Приложение должно иметь заголовок, который записывается симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами алфавита, начиная с А, кроме букв Е, З, Й, О, Ч, Ь, Ы, Ъ. Допускается обозначение приложения буквами латинского алфавита, за исключением букв I и O. Приложения выполняют на листах формата А4, А3, А4Х3,А4х4, А2, А1 по ГОСТ 2.301.

Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц. Все приложения должны быть перечислены в содержании отчета и с указанием их номеров и заголовков.

Документ подписан электронной подписью
Яковлев Алексей Николаевич
Ректор
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф. ГОРБАЧЕВА"

009639B77A14B5CACDBA0193FFB46793CA
Срок действия с 10.01.2023 до 04.04.2024
УЦ: Казначейство России

Подписано: 21.11.2023 09:38 (UTC+7)

1699402314